REMARKS

This Application has been carefully reviewed in light of the Final Office Action electronically mailed May 5, 2010. At the time of the Office Action, Claims 1-5, 7-10, 12-21, 23-26, 28-37, 39-42, and 44-60 were currently pending. Claims 1-5, 7-10, 12-21, 23-26, 28-37, 39-42, and 44-55 have been allowed. Claims 56-60 have been rejected. Applicants amend Claim 56 and respectfully request reconsideration and allowance of all pending claims.

Section 103 Rejections

The Office Action rejects Claims 56-60 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No. 2004/0123117 issued to Berger ("*Berger*") in view of U.S. Patent No. 7,539,664 issued to Dutta, et al. ("*Dutta*"). Applicants respectfully traverse these rejections.

Claim 56 recites a computer-implemented method for computer security, comprising:

> determining, using the central processing unit, quantitative information regarding the file for use in identifying whether the file should be added to a database of known good software, the quantitative information selected from the group consisting of a length of time the entry has been in the database of unfamiliar software, a number of times the file has been opened, and a number of times an executable in the file has been executed; [and]
>
> adding the entry for the file to the database of known good software if the quantitative information exceeds a predetermined value.

The Office Action states that the *Berger-Dutta* combination discloses these claim elements. *See* Office Action, page 3. However, the *Berger-Dutta* combination not only fails to disclose each of these claim elements, but it would not have been obvious to combine these references in the manner suggested by the Office Action.

The Office Action states that column 9, lines 34-43 of *Dutta* discloses determining quantitative information regarding a file. *See* Office Action, pages 4-5. *Dutta* relates to a "rating methodology for rating searches that are completed by peer nodes" in a peer-to-peer file sharing network. *See Dutta*, col. 8, lines 41-43. According to *Dutta*:

> The search result post-processor can monitor and record or log the number of times that a general file is opened or the number of times that an executable file has been executed. The search result post-processor could also monitor how long a file is kept before it is deleted.
>
> * * *
>
> If a retrieved file is used repeatedly by the user, then the ranking of the file for its one or more associated keywords is increased. If a retrieved file is kept for a relatively long period, then the ranking of the file for its one or more associated keywords is increased.

Dutta, col. 9, lines 37-49. Thus, this information regarding a file from *Dutta* is used to increase or decrease the rank of a file for use in a ratings system in a peer-to-peer file sharing network. Claim 56 has been amended to clarify that the quantitative information regarding the file is used for ***identifying whether the file should be added to a database of known good software***. Thus, the information regarding a file from *Dutta* is used for the completely different purpose of identifying popular or highly ranked files—there is no disclosure in *Dutta* regarding using quantitative information to determine whether the file should be added to a database of known good software.

Additionally, the Office Action states that *Burger* discloses adding an entry for the file to a database of known good software if the quantitative information exceeds a predetermined value. *See* Office Action, page 4. *Berger* actually discloses monitoring an application in a sandbox to determine if the application is safe, and updating a local configuration to reflect that a potentially unsafe application is now a known safe application. *See Berger*, pars. [0074], [0081]. Thus, *Berger* uses the behavior of the application in a sandbox to decide if an application is safe rather than comparing quantitative information with a predetermined value. In response to Applicants' previous arguments regarding this claim element, the Office Action states:

> Berger does in fact make the determination that an application is safe based on quantitative information value. See par. 32-33 and 75 that discloses monitoring and analyzing actions of the various applications executing on the system to detect malicious actions based on RULES.

Office Action, page 2. The Office Action then concludes that the rules from *Berger* are the same as the quantitative information recited by Claim 56. *Id.* at 2-3. However, the rules

from *Berger* are clearly different than the quantitative information recited by Claim 56. The rules from *Burger* include:

> (1) an action by an application that accesses the registry . . . (2) an action by an application that opens the application itself, e.g., an application that is mailing itself; (3) *an action that opens or alters many files of the same type, e.g., overwrites many bitmap or JPEG files*; (4) an action that modifies or deletes system files; (5) an action that opens unauthorized ports; (6) an action that attempts unauthorized communication over an open port; and (7) *an action by an application that opens any type of an executable file and modifies the executable file in a known malicious way.*

Berger, par. [0033] (emphasis added). The quantitative information recited by Claim 56 is selected from the group consisting of a length of time the entry has been in the database of unfamiliar software, a number of times the file has been opened, and a number of times an executable in the file has been executed. None of the above rules from *Berger* relate in any way to a length of time an entry has been in a database of unfamiliar software. Additionally, none of the rules from *Berger* include "a number of times the file has been opened." Although rule 3 from *Berger* relates to opening a file, that rule refers to the application that is being monitored opening *other* files, such as bitmaps or JPEGs. *Berger,* pars. [0032], [0033]. Claim 56, however, recites a number of times *the file* has been opened, referring to the actual file that is potentially unsafe. Finally, *Berger* has no rule based on a *number of times* an executable in the file has been *executed.* Although rule 7 from *Berger* relates an action by an application that opens an executable file and modifies the file in a malicious manner, this rule is not based on the number of times a file is executed, only whether a modification of a file is malicious. *Id.* at [0033]. Thus, the rules from *Berger* that are allegedly based on quantitative information are all different than the quantitative information recited by Claim 56. In addition, the only "rule" from *Berger* that is arguably based on any quantitative information that "exceeds a predetermined value" is rule 3 from *Berger. Id.* at [0033]. As discussed above, this rule is different from the quantitative information recited by Claim 56. Thus, *Berger* fails to disclose adding an entry for the file to a database of known good software if ***the quantitative information exceeds a predetermined value***.

Moreover, it would not be obvious to one of ordinary skill in the art to combine *Burger* and *Dutta* in the manner suggested by the Office Action. *See* Office Action, pages 4-

5. The Office Action acknowledges that *Berger* fails to disclose the specific quantitative information recited by Claim 56, and relies on *Dutta* as disclosing this quantitative information. The Office Action suggests that the allegedly quantitative information from *Dutta* should be used in conjunction with the malicious software detection from *Berger*. However, *Dutta* bears no relation to computer security and the quantitative information in *Dutta* is used for rating the popularity of a file. *See Dutta*, col. 9, lines 34-49. It would not be obvious to adapt *Dutta's* use of quantitative information for ranking the popularity of a file to *Berger's* determination of whether a file is potentially malicious. The Office Action states that the motivation for combining the references "would have been to improve the performance of malicious computer code detection as taught by Dutta et al (column 1, lines 5-10)." *See* Office Action, page 5. However, not only does this cited portion of *Dutta* have no relation to detecting malicious computer code, but the entire disclosure of *Dutta* is unrelated to detecting malicious computer code. *See Dutta,* col. 1, lines 8-13 ("[t]he present invention relates to an improved data processing system and ... provides a method and system for database and/or file accessing and searching"). In response to Applicants' previous arguments regarding the nonobvious *Berger-Dutta* combination, the Office Action states:

> Berger and Dutta are analogous in network monitoring and network data updating by making information current. Berger generates update to make the network information current, i.e. 'updates .... to reflect that the potentially unsafe application is now a known safe application. (see par. 57)' Dutta updates to make the network information current, i.e., 'updating ... throughout the peer to peer network (see col. 13 lines 55-59 & 63-67).'

See Office Action, page 3. Thus, the Office Action concludes that *Berger* and *Dutta* are analogous art because they both involve some aspect of network updating to make information current. However, this assertion by the Office Action is extremely broad, and ignores the fact that any updating in *Dutta* is done to alert the peer-to-peer network of the ratings of files, while any update in *Berger* functions to update a local configuration to identify safe and unsafe applications. *See Dutta,* col. 9, lines 34-49; col. 13, lines 55-59; *Berger,* par. [0057]. Thus, Applicants respectfully submit that it would not have been obvious to one of ordinary skill in the art to combine *Berger* and *Dutta* in the manner suggested by the Office Action.

Because the *Berger-Dutta* combination fails to disclose every element of Claim 56 and because it would not be obvious to combine the references in the manner suggested, Applicants respectfully submit that Claim 56 is patentable over the cited art and request that the rejection of this claim be withdrawn. Claims 57-60 each depends, either directly or indirectly, from Claim 56. Thus, for at least the reasons discussed above with respect to Claim 56, Applicants respectfully request that the rejections of Claims 57-60 also be withdrawn.

Conclusion

Applicant has made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other apparent reasons, Applicant respectfully requests full allowance of all pending Claims. If the Examiner feels that a telephone conference or an interview would advance prosecution of this Application in any manner, the undersigned attorney for Applicant stands ready to conduct such a conference at the convenience of the Examiner.

Although Applicant believes no fee is due, the Commissioner is hereby authorized to charge any required fee or credit any overpayment to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant

Chad C. Walters
Reg. No. 48,022
PHONE: (214) 953-6511

Date: July 2, 2010

CORRESPONDENCE ADDRESS:

Customer Number: **05073**